Anexo Corto - Requisitos de Seguridad de la Información (SI)

El Contratista acuerda maximizar la seguridad de sus personas, procesos y tecnologías a lo largo de la vigencia de este Contrato de conformidad con los requisitos establecidos en este Anexo y todas las leyes aplicables (colectivamente, los "**Requisitos de SI**"). La Compañía se reserva el derecho de validar la efectividad de los Requisitos de SI o el Contratista deberá proporcionar evidencia de una validación independiente por parte de un tercero, a solicitud de la Compañía. La Compañía podrá modificar los Requisitos de SI mediante notificación por escrito al Contratista. El término "producto", como se usa en este documento, significa cualquier servicio, equipo, sistema o software proporcionado por el Contratista a la Compañía en términos de este Contrato.

1 **Respuesta a Incidentes y Notificación de Filtraciones**. El Contratista acuerda que cualquier filtración o cualquier otro incidente de seguridad, interno o externo, que pueda comprometer múltiples fuentes de datos, deberá informarse al Centro de Operaciones de Seguridad de la Compañía (soc@sempra.com (858) 613-3278) dentro de las 24 horas a partir del conocimiento de la filtración, seguido de un de plan de remediación de 72 horas, y 2 semanas hábiles a partir de la notificación inicial para completar la investigación.

2 **Cifrado**. Cuando la Compañía determine que el cifrado es aceptable para evitar la divulgación no autorizada de la información de la Compañía, para proteger la información sensible de la Compañía, los productos del Contratista usarán controles criptográficos que satisfacen los requisitos de FIPS 197 de tal manera que los datos e información sensible de la Compañía sean inaccesibles por un usuario no autorizado. Cuando el producto del Contratista utilice llaves de cifrado, el producto del Contratista no almacenará las llaves de cifrado dentro del código fuente. Las llaves de cifrado se almacenarán y protegerán por separado del producto mientras estén en tránsito y en reposo, y serán revocables para su reimplementación y mantenimiento.

3 **Seguridad de los datos.**

a. Capacidad de bloqueo/restricción. En caso de que se sospeche o se produzca una violación o compromiso sospechoso o real que involucre la infraestructura del Contratista, esté o no relacionada con el producto, la Compañía podrá, a su entera discreción, bloquear o restringir todos y cada uno de los métodos y fuentes de acceso del Contratista, incluyendo, sin limitación, la comunicación, la conectividad y las integraciones (colectivamente, "Derecho de bloqueo"). Sin perjuicio de cualquier otro requisito u obligación de la Compañía en el presente Contrato, si la Compañía ejerce su Derecho de Bloqueo, la Compañía no tendrá ninguna responsabilidad hacia el Contratista que surja o esté relacionada de alguna manera con el mismo. El acceso requerido del Contratista sólo se restablecerá después de que el Contratista haya demostrado efectivamente, a través de un tercero independiente y competente, que su producto y los sistemas relacionados ya no representan una amenaza potencial o real para la Compañía.

4 **Destrucción**. El Contratista acepta que, cuando se haya superado el período de retención de los datos, cuando los datos ya no sean necesarios, o a petición de la Compañía, el Contratista destruirá los datos de una manera que los hará completamente inutilizables e irrecuperables, y proporcionarán a la Compañía un certificado de destrucción, a solicitud de la Compañía.

5 **Conflictos**. Nada de lo contenido en este Contrato se interpretará como una limitante de cualquiera de las obligaciones del Contratista en materia de no divulgación o protección de la información contenidas en otras partes de este Contrato, incluidos, entre otros, los términos y condiciones contenidos en el cuerpo principal del mismo.